INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 10, Issue 5 - V10I5-1405)
Available online at: https://www.ijariit.com

Streamlined Attendance Monitoring: Multifaced Recognition

Makineni Saroj Vihung
sarojvihung@gmail.com
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad

Kanduri Sahith
kandurisahith02@gmail.com
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad

Baddam Rithika Reddy
rithikareddy.baddam2004@gmail.com
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad

Samala Keerthi
skeerthishetty0309@gmail.com
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad

Savarapu Omkaarini
omkaarini2003@gmail.com
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad

Thirupathi Nanuvala
thirupathi_n@vnrvjiet.in
Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering &Technology, Hyderabad

ABSTRACT

To precisely discover human beings, conventional attendance structures normally depend on biometric techniques like fingerprint or iris scanning. But these systems frequently have scalability and performance problems, especially while handling large companies straight away. This research gives a novel technique to decorate attendance monitoring through using ultra-modern multi-face popularity techniques. In assessment to conventional biometric systems which are commonly restricted to unmarried user processing, our device can effortlessly control several customers immediately. It makes use of a combination of several algorithms to detect spoofing, become aware of faces, and perform excessive-precision recognition. By integrating these techniques, the system overcomes common issues associated with traditional techniques, such as false identities and unauthorized access, and provides a robust solution provide accurate and reliable attendance records This method not only provides accurate and speedy attendance tracking but also ensures the integrity of the process Becoming an ideal solution for environments that require biometric identification systems.

KEYWORDS: *Face Recognition, Multi-Face Detection, Haar Cascade Classifier, Face Net Model, Anti-Spoofing, Convolutional Neural Network (CNN), Attendance System, Machine Learning, Computer Vision, Image Processing, Real-Time Processing.*

INTRODUCTION

The development of a multi-face reputation attendance device marks a substantial improvement in attendance monitoring generation, permitting the simultaneous identity of a couple of people. By employing ultra-modern device mastering and pc vision algorithms, the device achieves amazing scalability, accuracy, and overall performance, even under difficult conditions collectively with numerous lighting fixtures and several facial expressions. The tool's structure includes a multi-stage system starting with a Haar Cascade classifier for quick and robust face detection, making sure that only the relevant facial areas are similarly analyzed. The next use of the FaceNet version lets in for the generation of specific facial embeddings, permitting specific reputation of a couple of faces inside a single frame.

Security is one of the most important aspects of this system since a Convolutional Neural Network (CNN) has been implemented in order to detect fraudulent presentation attacks which further safeguards this system from any unauthorized access.

The performance of the system is put to thorough testing and experimental verification proving it is fit for use in many sectors such as education, business, and other areas where efficient and advanced biometric systems are required.
Most importantly, the system is also developed with the user and privacy in mind. This means that the portal is user-friendly during enrolment and attendance data is accessible for the administrators in real time, all this while observing the data protection policies. This aspect not only improves the precision and efficiency of attendance management systems but also redefines the limits of biometric identification systems in fast changing environments.

MODULES IN MULTI FACE RECOGNITION SYSTEM

Face Detection

When individuals come in front of the camera, the system instantly recognizes their faces with the necklace and draws protective boxes around them to isolate facial regions for further analysis. Haar Cascade begins with the concept of Haar components, which are simple rectangular objects used to capture changes in energy in an image. This necklace wave-generator is designed to represent shapes such as edges, lines, squares, etc. by calculating the difference in intensity differences between different regions of the image This calculation works well by using integral imaging, enabling rapid estimation of necklace features in different regions of the image.
To identify the most suitable Haar products, Haar Cascade uses the AdaBoost algorithm, a machine learning technique that combines multiple weak classifiers to create a more complex classifier. It assigns weights to these factors and trains classifiers based on weighted importance. The final classification is a weighted combination of these weak distributions, optimized to minimize classification errors.
The search algorithm uses a series of hierarchical categories. Each stage of the cascade consists of a classifier trained to distinguish between regions where an object is present and where it is not. At the beginning, a simple classifier with low features is used to quickly discard regions that are unlikely to contain features. As the cascade progresses, the classifiers become more complex, use more features, and improve visibility. This hierarchical approach ensures efficiency by placing computer hardware in promising locations.
During the search, the image is scanned with a sliding window. Each window is searched using a cascade of classifiers, and windows are classified based on whether cascade contains or excludes features.
All windows occupying parts of the cascade are marked as containing the object. This method is very efficient, suitable for real-time applications, capable of detecting objects even under different conditions such as different lighting and conditions.

Face recognition

When a face is diagnosed, the process of reputation commences through the FaceNet model. In the simple phrases ‘face recognition: FaceNet’ is composed of various ranges and contains the concepts of deep mastering for progressed recognition performance’. To start with FaceNet applies a deep CNN for facial photo analysis. This community is eove skilled to fit the above mapping in exercise, i.E., to educate the above referred to network even earlier than the mapping is to be had, furnished that the network has get admission to to a huge series of face photos. In particular for the duration of the schooling method, the network is taught to differentiate the distinctive aspects of a face that can be used to describe a particular individual. These are later used as the wonderful traits of a specific character. Such feature vectors also are referred to as embeddings, which tend to % near in the Euclidean area for faces which might be alike, however are separated for faces that are not.

The training is carried out with the use of a loss function, particularly, triplet loss, that's used in this situation. This method compares 3 images inside the shape of anchor, fantastic and poor pics. The anchor image is where all the other images are compared to and the high-quality photograph is a picture of the same man or woman because the anchor but at a distinctive example and negative photograph indicates a specific man or woman. The most important goal here is to deliver the anchor and the fantastic embeddings near and the anchor and poor embeddings some distance away. Repeating this for lots of these training samples, the community is capable of examine techniques which form clusters for faces of the identical man or woman and create massive gaps in among clusters from special people.

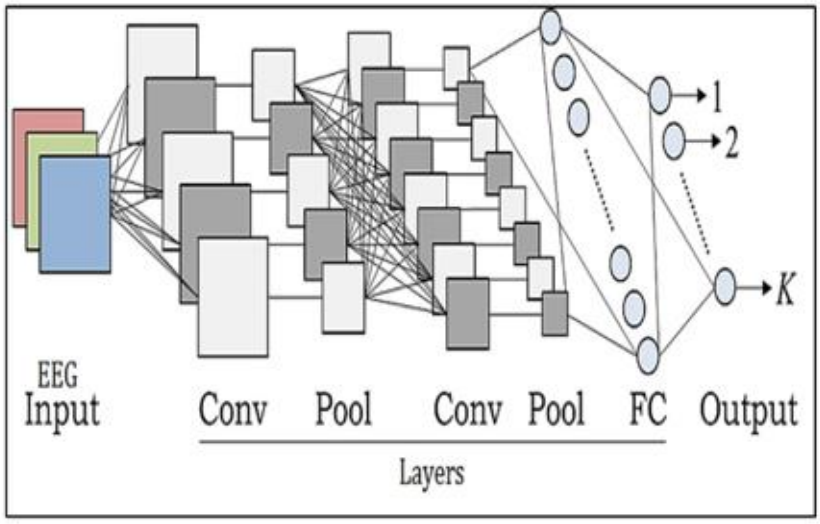
As part of the process, the input face photograph is put through the trained FaceNet model to get its embedding. This embedding is then compared to a face embed database with a known metric of similarity, commonly cosine similarity or Euclidean distance. The system recognizes the person whose face - known and stored in the database - has the embedding that is the nearest to the eyewitness face’s embedding. These features make it possible for FaceNet to carry out fast and reliable face identification under varying defying conditions such as lighting, pose, and even expression.

First, the performance and scalability of the FaceNet deserves particular emphasis. The embedding space created by FaceNet is highly discriminative, that is, even small variations among faces are captured quite well. This feature, in turn, enables FaceNet to efficiently perform large-scale face recognition. Furthermore, the embeddings can also be applied in other tasks aside from face recognition, which include face verification and face clustering thus making FaceNet a useful application in computer vision.

Anti-spoofing model

While making use of a Convolutional Neural Network (CNN) for classification purposes to test if an photograph is fake or real, there are gravitating levels to the manner to resource in solving the problem of figuring out real pics and pictures spoofed and supplied to the machine.
The technique starts by using the CNN looking for factors in the target photograph via numerous convolutional layers. Each convolutional layer locations small filters over the photograph that scan for easy shapes like edges or textures, or more complex shapes like styles.

When one of the purposes of the detection machine is to detect spoof, such layers are used to offer signs and symptoms of manipulations consisting of the presence of unnormal textures or disturbances in the pics that are typically supplied to the machine in preference to the scanned man or woman.
The convolutional layers start off very basic and simple, then with the increase in the level there are higher and more complex levels of abstraction developed features, which allow the network to look at the differences between real images and the fake ones.



After the completion of feature extraction, the next immediate step is the spatial dimension reduction of the feature maps by use of max pooling layers within the CNN. Max pooling eliminates the inconvenience associated with feature maps by picking out the peak values from certain sections, which is also aimed at promoting the concentration on important characteristics while at the same time easing the computational burden. This diminishment is essential because it helps in managing the data and avoiding the problem of the network being flooded with unnecessary information that does not assist in the spoofing detection task.

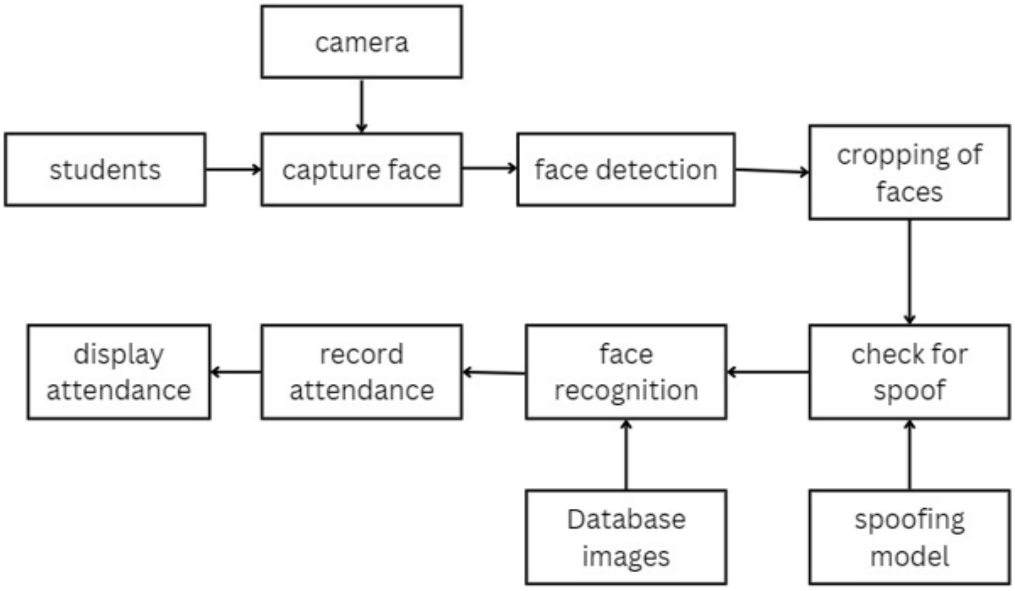
An Adaptive Average Pooling layer acts as a second image dimensionality reducer and maintains a constant input for the next layers irrespective of image variations. This layer changes the output feature maps to a predetermined size such as 4x4 pixels regardless of the input image size. This helps in normalizing the processing images of varying sizes within the network architecture thus in enhancing processing of the images during the last classification phase.

During the last classification phase, the processed features are inserted into so-called fully connected layers. They put the features together and interpret them to argue how likely the image is real and how likely it is a fake one. The final fully connected layer gives predictions about all the existing classes (here, a class that depicts a real person used a sigmoid function and a class that shows a fake person used a different function). This feature allows the network to be able to classify an input image of a live person and an image of a photograph or video, and it can also discriminate between a real and fake image The incorporation of a careful observation of what pattern and faults depict spoofing will help the CNN give correct classifications. This classification ability makes these networks an asset in addressing the problems of security and reliability in face recognition systems.

ARCHITECTURE
The multi-face recognition attendance system has been earnestly developed for better management and the security of attendance tracking by employing modern machine learning and computer vision techniques. It consists of a number of functions executed in the order they help in high precision and reliability of the whole procedure.

The first step of the system is an image capture, a phase whereby a camera is fixed and pointed at the entrance of the classroom and students are continuously photographed as they enter the room. The camera in this case acts as the main imaging device and provides live feeds which will be needed in the entire system for most periods. The images fed to the system should be of good quality since the ability to find and recognize faces in the later stages depends on this stage.
After the stage of image capture, Within the System using Face detection system, Haar Cascade Classifier is used to locate and Detect the human faces present in the image. This algorithm is selected due to its speed and strength that allows the system to perform a rapid scan of the image and resolve the facial regions with a high accuracy rate. By doing so, only the facial regions of interest are included in the processing, thus reducing the processing time without excluding any important facial features that need to be processed further.

After the facial areas are recognized, the system then goes to the step of cropping the areas in order to concentrate only on the facial components. These cut out facial images are then put through an intensive security scrutiny. The system amolies a Convolutional Neural Network model with anti-spoofing capabilities. This model processes images to ascertain whether the presented face is real or a spoof attempt; for instance, a picture or a video displayed to the system in an attempt to cheat it.
It is an important step in soliciting the authenticity of attendance records because it deters any form of impersonation through attendance faking using images or videos.



Once the validity of the faces is assured, the system proceeds to the stage of face recognition. At this point, it utilizes the FaceNet architecture to compute the corresponding unique face embeddings for every face visible in the image. When operating, FaceNet is such that faces are embedded in a high dimensional space and the distance between any two embedded points is related to the similarity of the faces. With this technique, the system can recognize and tell apart several faces within the same photograph. The FaceNet facial embeddings are then matched with the existing ones in the computer system, making it possible to identify each one exactly.
Finally, after the recognition of the faces in the images, attendance information is recorded by the system. The attendance of persons whose identities have been established is recorded without delay and can be accessed by the administrators right away using the system's interface. Then, attendance lists are presented by the system, which means that there is always an indication of the individuals who have been identified and marked present. This entire exercise not only reduces the time and improves the efficiency of attendance registration, but also increases the level of protection against abuse due to the installed systems aimed at detection of such behaviour.

TRAINING MODELS

In the image processing system of face recognition, a pre-trained FaceNet model is first loaded to generate face images embeddings. Face detection in images is performed with the first step of employing Haar Cascade classifier. The face region is then cropped and resized to the expected input size of the Facenet Model.
These processed face images are fed into the FaceNet model producing up to four unique face embeddings of 128 dimensions each for each face image. A list is kept for all such embeddings in which the face embedding is indicated against the file name of that face. This list is also done for storage purposes.
Within the model, its convolutional architecture possesses five convolutional layers of which the purpose of each is to extract more and more advanced and abstract features from input images. The first Convolutional layer comprises of 32 filters that are used to identify fundamental features such as lines and textures. It deals with very basic features involving a few elements such as lines and gradients, which are the most basic structures of any complex design. The filters in this layer scan the image and capture low-level features of the input without any focus on the specific part of the image.

Consequently, the second convolutional layer, consisted of 64 filters, features also in using a few complex combinations, in addition to the basic features presented by the first layer. This layer is capable of distinguishing between shapes, corners, and all other basic features that help develop a structure of the human face. This however means that the number of those beginning filters is increased and thus the representation of those features becomes denser, making the understanding of the face much more complex.
As we proceed to the third convolutional layer consisting of 128 filters, it can be noted that more complex patterns are recognized by the model. The combination of features from the first two layers allows this layer to identify textures or patterns such as portions of the face, which suggest whether the face is real or it is being faked.
In the 4th convolutional layer with 256 filters, the highly abstract features are extracted. At this point in time, the model is capable of computing specific face spoofing minute details explained by the textures of skin and lighting patterns among others that can be used to tell whether the face is being spoofed. This layer being the deepest focuses more on such detailed indicators which helps the model to distinguish between a real face and a fake face even to a greater level.

Eventually, 512 filters are used at the given fifth convolutional layer to detect the most abstract and complex structures. This layer integrates all features acquired in previous layers providing an adequate representation of a very high level necessary for differentiating real and spoofed faces. The output, after undergoing this process, is passed through an adaptive average pool layer which ensures the following fully connected layers, that make the final classification, are of the same size.
The entire training process comprises a total of 50 epochs with each epoch being one complete iteration of the training set. In other words, the model in the course of each epoch goes through all the training images in the form of batches and adjusts the weights after every batch according to the computed loss for that respective batch.

The purpose of this is to reduce the gap between what the model predicts and what the actual labels are. During training, even within these epochs, the model's weights are fine-tuned and thus its ability to differentiate between a real image and a spoofed one improves over time.
By the end of the training process which consists of 50 epochs, the model is now expected to have been learned how to generalize on different face images and tell if a face is real or fake.

OBJECTIVE

The prime objective of the current endeavour is to build an attendance system, which can agreeable scale up and exude trustworthiness, owing to the use of advanced multi-face recognition technology in attendance systems that will resolve the shortcomings of traditional biometric methods like fingerprint or eye iris scans. Its true that traditional systems have their benefits however they often pose a problem regarding scalability and efficiency especially with real-time systems for a large population. Due to their very configuration, they are designed to work on one person at a time which makes them inappropriate in cases that require quick identification of many individuals. More so, such a system is susceptible to other gremlins such as identity theft and unauthorized attendance that can distort the accuracy of the attendance system records.
This research paper is meant to present a better appreciation of multi-face identification technology in learning institutions through an attendance monitoring system. The system is designed in such a manner that it aims at the limitations associated with the use of conventional biometrics and offers a reliable, Nomadic, and efficient alternative that can be applied in various situations with high attendance accuracy needs. This treatment ensures and protects the entire system while enhancing attendance records accuracy through sophisticated detection, recognition, and anti-spoofing strategies.

AREA FOR FUTURE WORK

As a last step in improving the face anti-spoofing model, enlarging the dataset with more facial images and spoofing techniques will likely make the model more durable. For example, including the use of images created by GANs or using 'adv. attack' would be creating situations that are more difficult and hence, require the model to be more versatile in handling different attacks. This variety of data would promote the application of the model in real-life situations where a new way of spoof may be presented.
Exploring more complex model architectures like ResNet and EfficientNet might also contribute to the enhancement of the outcome. These architectures have been proved better than others in the performance of the feature extraction and classification tasks, due to their more in-depth and improved network configurations. Moreover, the use of transfer learning can make it possible to exploit features from existing model, thereby making it possible to achieve better performance in shorter time especially when adequate labelled data is not available.

Another critical area for the future is real-time deployment of the model. The model can also be modified for less cumbersome computational needs through pruning, quantization, etc. This would make it deployable for edge devices like smartphones or even embedded systems, thus allowing practical use cases for example in mobile secured authentication when instant and accurate spoofing presence detection is a must.
A combination of multiple modalities in detection can also enhance the overall anti-spoofing system. In addition to face recognition, more biometric modes such as voice or eye iris, or even behaviour would be used in this system for enhanced security. This means that the system would not focus on detecting simulation with one mode, which would make it difficult to spoof the system in use.

EXPERIMENTAL SETUP AND RESULTS

Experimental Setup

The testing configuration for this project uses a pre-trained FaceNet model for anti-spoofing detection and facial identification. OpenCV is used for face identification, while FaceNet embeddings in real-time video feeds or image processing are used for face confirmation. The technology ensures that attendance is only recorded for genuine faces by separating real and phony faces by comparing the current camera input with stored embeddings. The accuracy of the model is maximized by training and testing it on datasets containing both real and false photographs.

Environment Configuration

- Operating System: Windows 10
- Programming Language: Python 3.7+
- IDE: Visual Studio Code

Libraries:

- ***TensorFlow and Keras*:** Used to build and train the CNN models
- ***OpenCV and Pillow*:** Used for image processing
- ***Numpy*:** For handling arrays and matrices, crucial for model input/output processing.
- ***Sklearn*:** For evaluating model performance with such accuracy ,precision.
- ***Keras-Facenet*:** Keras-Facenet is a high-level deep learning library built on TensorFlow, offering pre-trained FaceNet models for efficient face recognition and embedding generation.
- ***Facenet-Pytorch*:** Facenet-PyTorch provides a PyTorch implementation of the FaceNet model, designed for easy integration and optimized for face recognition tasks using deep learning techniques.

RESULTS

A facial recognition system for anti-spoofing and attendance tracking is shown in figures 7.2.1 and 7.2.2. The technology is able to discern between fake and real faces in both scenarios. It identifies two spoof faces on a smartphone screen as "Spoof" and highlights them with red bounding boxes in Figure 7.2.1, whereas it recognizes a real face, "Saroj," indicated by a green bounding box. The method uses red bounding boxes to mark all four faces on the mobile screen as "Spoof" in Figure 7.2.2. This illustrates how the system works to prevent the use of photos or videos for spoofing by ensuring that only real, live faces are accepted for procedures like attendance.

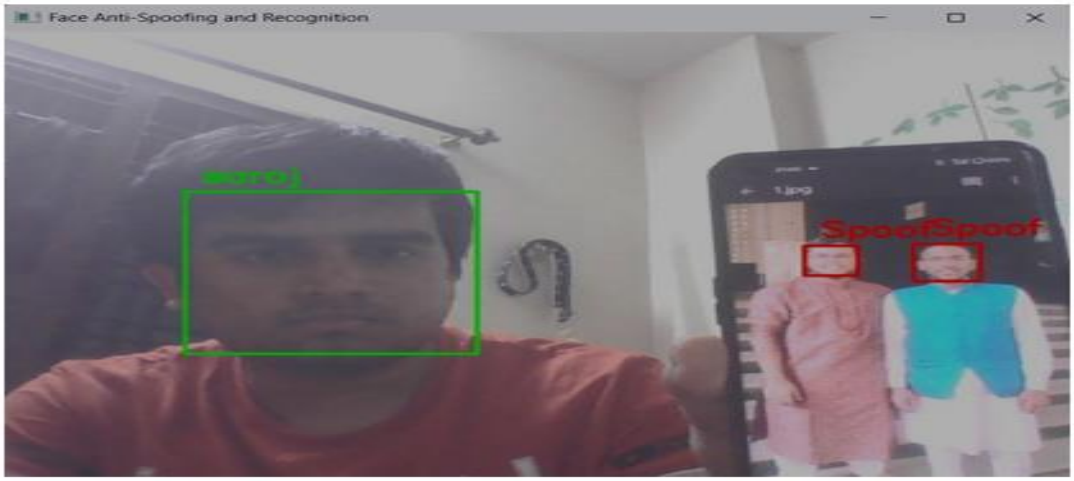


Fig 7.2.1: Live Camera Face Detection

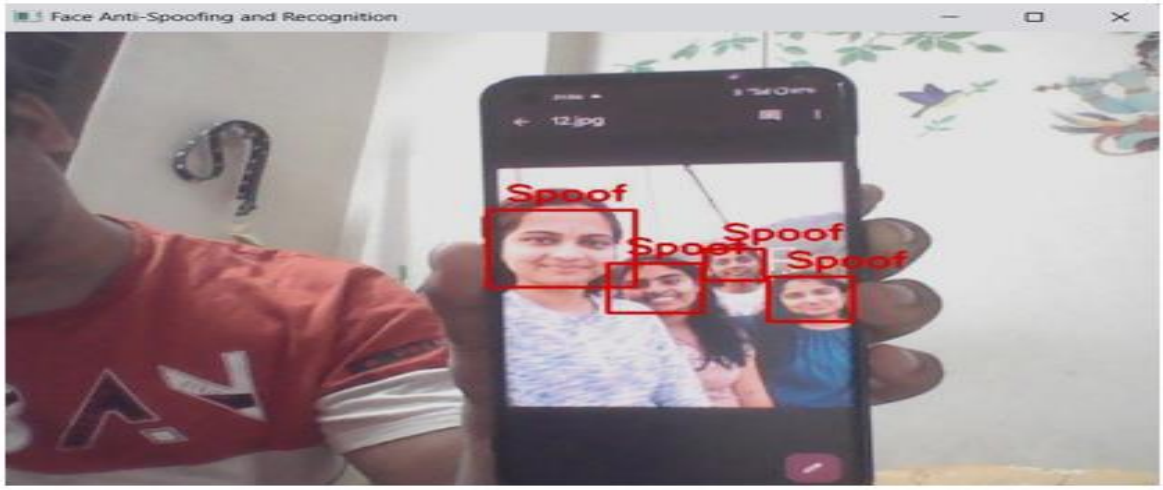


Fig 7.2.2: Spoof Image Detection Results

In fig 7.2.3, only one person, "Saroj," is recognized as real, with a green bounding box around their face, indicating that attendance will be marked for them.

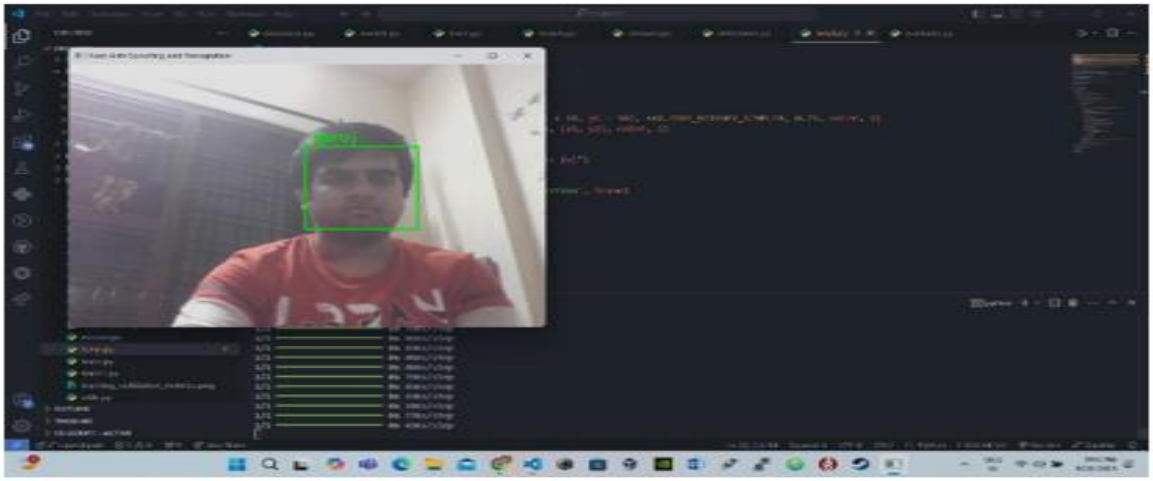


Fig 7.2.3: Single Face Detection

Fig 7.2.4, two individuals, "Rithika" and "Omkaarini," are identified as real with green bounding boxes, meaning their attendance will also be recorded.

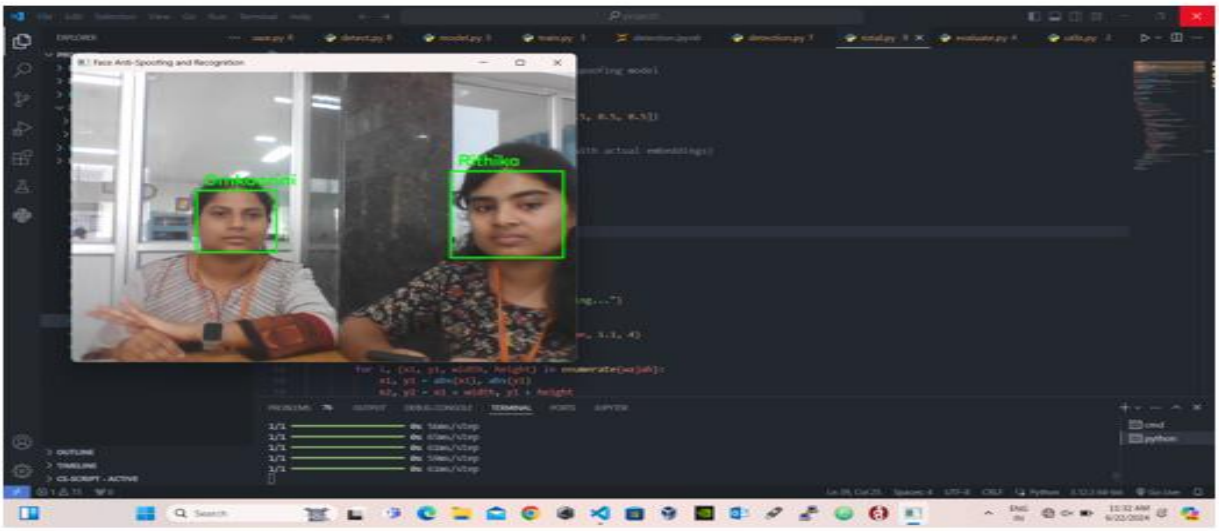
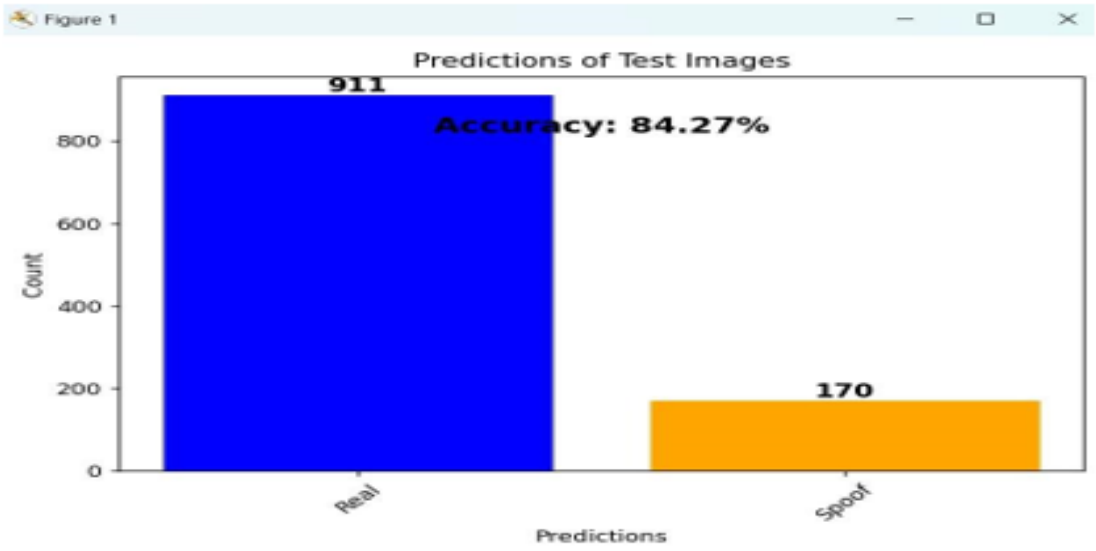


Fig 7.2.4: Multi face detection results

Bar Graph:
The prediction result of the test images is visualized in bar graph, by comparing the real and spoof faces. The blue bar corresponds to 911 real images and orange bar corresponds to 170 spoof images. Overall accuracy of 84.27% which predicts the real /spoof label close to the ground truth, indicates that the number of real images correctly predicted is higher in number which means it has very high discriminative capability between real/spoof faces.

CONCLUSION AND FUTURE SCOPE
This research provides an efficient method for automating attendance systems using state-of-the-art computer vision algorithms. Through the integration of FaceNet, Haar Cascade, and CNN anti-spoofing, it provides accurate and secure person identification. While Haar Cascade offers a fast and reliable real-time face detection technique, FaceNet generates highly discriminative embeddings for precise recognition. CNN anti-spoofing is used to ensure that only real, live faces are recognized, preventing any bogus efforts to record attendance. Security is greatly increased by doing this.



The proposed method effectively addresses common problems with face recognition-based attendance systems, such as lighting variations, variations in facial expressions, and attempts at system spoofing. In situations where maintaining track of student attendance is essential, these technologies cooperate to guarantee accuracy and security.
The foresight of a multi-face detection system inspires confidence particularly in situations that are very complex such as, looking at, detecting identical twins, faces hidden by masks, and very bright lights. One of the main difficulties that will be addressed is that of recognizing beautifully identical twins. Such systems would be equipped with enhanced algorithms employed in feature extraction that is not limited to facial features but also includes many details like textures of the twin's faces, colors, and even the movement of the eyes and skin. Furthermore, behavioral biometrics such as voice, gait, or gesture analysis could also be implemented alongside facial recognition to create a multi-layered recognition system. This would also help when twins are present in the identification system. In excessively lit environments, some safeguard against this is advances in infrared-based identification

systems or more novel adaptive image processing systems capable of adjusting for lighting influencing the performance of the system. Such developments would significantly improve the strength, accuracy and applicability of multi-face detection systems.

REFERENCES

[1] S. Hapani, "Automated Attendance System Using Image Processing," in Proceedings of IEEE Conference on Automated Systems, 2023.
[2] S. Sathyanarayana, "Automatic Student Attendance Management System Using Facial Recognition," in International Journal of Emerging Trends in Computer Science and Engineering (IJETCSE), 2023.
[3] N. Kanchan, "Attendance Management System Using Hybrid Face Recognition Techniques," in Proceedings of IEEE Conference on Hybrid Recognition Techniques, 2023.
[4] S. Chintalapati, "Automated Attendance Management System Based on Face Recognition Algorithms," in Proceedings of IEEE Conference on Face Recognition Algorithms, 2023.
[5] E. Vardharajan, "Automatic Attendance Management System Using Face Detection," in Proceedings of IEEE Conference on Face Detection Systems, 2023.
[6] "Face Recognition Attendance System Using Machine Learning and Deep Learning," in Proceedings of the Conference on Machine Learning and Deep Learning Techniques, 2023.
[7] "Intelligent Attendance System with Face Recognition Using the Deep Convolutional Neural Network Method," in Proceedings of the Conference on Deep Convolutional Neural Networks, 2023.
[8] "Automatic Attendance System Using Face Recognition Technique," in Proceedings of the Conference on Automatic Systems Using Face Recognition, 2023.
[9] "Face Recognition Attendance System Based on Real-Time Video Processing," in Proceedings of the Conference on Real-Time Video Processing, 2023.
[10] "Deep Facial Recognition Using TensorFlow," in Proceedings of the Conference on TensorFlow for Facial Recognition, 2023.
[11] "Face Recognition-Based Lecture Attendance System," in Proceedings of the Conference on Lecture Attendance Systems, 2023.
[12] "Face Detection and Recognition Using the Viola-Jones Algorithm, Principal Component Analysis (PCA), and Artificial Neural Network (ANN)," in Proceedings of the Conference on Face Detection Algorithms, 2023.
[13] "Appearance-Based Facial Detection for Recognition," in Proceedings of the Conference on Appearance-Based Detection Techniques, 2023.
[14] "Algorithm for Efficient Attendance Management: Face Recognition-Based Approach," in Proceedings of the Conference on Efficient Attendance Management Algorithms, 2023.